



U.S. Department of Justice

*United States Attorney
Eastern District of New York*

SK/JAM/AFM
F. #2016R02228

*271 Cadman Plaza East
Brooklyn, New York 11201*

October 4, 2021

By ECF

The Honorable Eric R. Komitee
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, NY 11201

Re: United States v. Aleksandr Zhukov
Criminal Docket No. 18-633 (S-1) (EK)

Dear Judge Komitee:

The government respectfully submits this letter in connection with the sentencing of the defendant Aleksandr Zhukov, scheduled for October 15, 2021.

From half a world away, the defendant built a massive datacenter botnet and used that botnet to perpetrate a multi-year cybercrime and fraud scheme that swindled U.S. companies in the digital advertising industry and siphoned millions of dollars out of their bank accounts and into the defendant's. In doing so, the defendant did what he had done so many times before—he gambled. He decided to lie, cheat, and steal from American companies and bet that he would never be brought to an American courtroom to answer for it.

Too many international cybercriminals take the same gamble, and there is a tremendous public interest in deterring them. Schemes like the defendant's cause financial losses to hundreds of U.S. companies, impose hardship on legitimate businessmen and women forced to operate at their own risk and without recourse, and undermine trust and confidence in online transactions. Criminals like the defendant who manage these criminal enterprises hide behind keyboards in foreign countries and are careful to avoid putting themselves at risk of extradition. They use increasingly sophisticated tools and techniques to obfuscate their true identities and their technical and banking infrastructure is frequently scattered across multiple international jurisdictions, making it difficult to obtain relevant evidence and recoup losses. Identifying cybercriminals such as the defendant and bringing them to justice requires a substantial commitment of law enforcement resources. In light of the success of law enforcement in dismantling this cybercrime ring, it imperative to deter this

defendant and other potential cybercriminals by sending a clear message that they risk severe consequences if they choose to target the United States.

For the reasons set forth herein, the government respectfully requests that the Court impose the Probation Department's recommended sentence of 15 years' imprisonment.

Background and Offense Conduct

The government realizes that the Court is already familiar with the offense conduct in this case, having presided over the four-week trial. An overview of the offense conduct is also set forth in the Presentence Investigation Report ("PSR"). See PSR ¶¶ 7-36. The following sections are therefore intended to provide only a high-level overview of the basic facts of the crimes for which the defendant was convicted. Those crimes consisted of the conspiracy to defraud brands, ad platforms, and others in the digital advertising industry (Count One), the conspiracy to raise money for and launder proceeds from that scheme (Count Three), and substantive wire fraud and money laundering conducted in carrying out the scheme (Counts Two and Four).

Between September 2014 and December 2016, the defendant carried out a digital advertising fraud scheme known as Methbot. The defendant was the undisputed leader of the scheme. GX 667T (defendant was "Project Owner"). He recruited more than half a dozen computer programmers and other employees to help him perpetrate the scheme and build up the technical infrastructure required to create fraudulent ad traffic. He provided these individuals with direction, referred to them as "my developers," and kept a 75% share of the scheme's proceeds for himself.

The defendant operated his scheme under the name of his purported ad network, Media Methane. Media Methane had business arrangements with other advertising networks that enabled it to receive payment in return for placing advertisements—primarily video advertisements (or "pre-rolls"). The defendant registered the website for Media Methane, paid for business registration and domain reputation services to make it appear more legitimate, and enlisted a copywriter to fill the website with content. Through the website, the defendant falsely represented to others that Media Methane was a Video Ad Network that would help "broadcasters and publishers reach consumers," find the "perfect audience," and deliver ads "to the right customer at the appropriate time." GX 1101. He further falsely represented on his website that, "All the traffic is controlled by such filters as IAS and Forensiq therefore our publishers get only quality and proven customers." GX 1101. During the scheme, the defendant directed others to the Media Methane website. GX 1699; GX 2110. He also communicated with others from his Media Methane email account, and using "Media Methane" in his signature block, to advertise his false goods as real. For example, on October 15, 2016, the defendant sent an email to a potential business partner in which he stated (falsely): "We still have a lot of USA traffic perfectly for prerolls, all traffic good scored by IAS, DV, WhiteOps, MOAT, etc .. we do about 40-50 millions HQ USA impressions daily." GX 1684T. He continued to make similar representations through December 2016.

Rather than place advertisements on real publishers' webpages as promised, however, the defendant rented approximately 2,000 computer servers located at commercial datacenters in Dallas, Texas and Amsterdam, the Netherlands, and programmed the datacenter computer servers ("bots") to simulate humans viewing ads on webpages. The defendant and his co-conspirators programmed the bots to load real ads on blank webpages, but represented that the ads were loading on the webpages of more than 6,000 publishers, including The New York Times and the New York Post.

The defendant and his co-conspirators also programmed the bots to appear and behave like human users, to deceive fraud detection companies (and the advertisers, publishers, and platforms that hired them) into thinking the bot traffic was in fact human traffic, and to thereby prevent the traffic from being blocked and ensure later payment for the ad impressions. To this end, the defendant and his co-conspirators programmed the bots to falsely represent that they had screens and mice, falsely represent that they were running operating systems used for personal computers (Windows and Mac) when they were in fact running an operating system used for datacenter computer servers (Linux), falsely represent that they were running commercially available internet browsers (Chrome, Firefox, Internet Explorer, Firefox) when they were in fact running a custom-made automated browser created by the defendant and his co-conspirators (the Methanum browser), bypass captchas, accept cookies, and falsely appear to be signed into the popular social media services Facebook, Twitter, and Google. The defendant and his co-conspirators also programmed the bots to click around a screen a randomly determined number of times, simulate a mouse moving around and scrolling down a webpage, and control and monitor video playback, including the length of time the video was watched.¹

In addition, the defendant registered the IP addresses associated with his bots in the names of major U.S. internet service providers. See GX 508, GX 509, GX 510, GX 511. For example, the defendant infiltrated the global WHOIS database through the AFRINIC registry and registered his bots' IP addresses in the names of "Comcast Cable Communications, Inc.," "Time Warner Cable Inc.," "Verizon Trademark Services LLC," "AT&T Services, Inc.," "Cox Communications Inc.," "Charter Communications Operating, LLC," "Cequel Communications Holdings," and "CenturyLink, Inc." GX 525A. The defendant also directed that IP addresses be registered in false corporate names that might be mistaken for home internet providers, including "Home Internet Orang LTD," "Dallas online LTD," "Verison Home Provider LTD," "AmOL wireless Net," "Chicago Air Online," "HomeChicago Int.," "CH wireless," "ATOL Intertnet," "Speed Home Internet LTD," and

¹ This included software features and code specifically designed to deceive the fraud detection firms DoubleVerify, Forensiq, Integral Ad Science, TubeMogul, FraudLogix, MOAT, SpringServe, and WhiteOps, and the U.S. companies that were the clients of those firms.

“US online LTD.” GX 525B through GX 525K. In this way, the defendant misled others that the computers in question belonged to customers of these internet service providers, rather than being located in datacenters. The defendant also entered false usage and location information into IP databases like MaxMind—a database that, like WHOIS, is widely relied upon in the industry—to make it appear that the computers in question belonged to real human internet users located in homes and businesses around the country.

The defendant’s various communications with his co-conspirators provide a real-time narration of the scheme. For example:

- On or about July 2, 2014, the defendant told a criminal associate: “I really need money;”) “just for a living).” The two individuals then discussed in detail how to make money through ad fraud with bots. Zhukov explained: “our idea is that we’ll get a lot of browsers on a Dedicated server and complete emulation, including mouse moves, and through sockets we’ll change the IP address on each browser.”
- On or about July 10, 2014, when asked how he came up with the idea for Methbot, the defendant told a criminal associate: “It’s simple. While I was drinking I realized that I need money ASAP) and since I am an experienced scam artist/adventurer, I immediately started thinking about how I could screw everyone one more time) and I succeeded).”
- On or about September 18, 2014, the defendant continued discussing his scheme and during the course of the conversation stated that he was the “king of fraud!”
- On or about October 28, 2014, the defendant instructed a co-conspirator to address the “lack of mouse move,” an undertaking that continued over the following year.
- In January 2015, the defendant boasted to an associate: “we have our own solution which allow us cross all known checkers and filters . . . it is clever server bot which can do absolutely anything .. watch video, click prerolls, show IAS traq score +700 etc.”
- In a to-do list dated June 25, 2015, the defendant instructed one of his programmers to address “complaints about fake Chrome and mouse move” and cause the datacenter computer servers to appear to be signed into Facebook: “add authorization for facebook authorized users. There is Google, twitter, too; no FB (there should be approximately 40% of them).”
- On or about August 4, 2015, the defendant wrote a note to himself titled “ROADMAP” that indicated that after his “Pre-roll launch,” his plan involving

“monitoring DVForensik filters for the possibility of fucking them over like with Google or IAS scheme.”

In September 2015, the defendant and one of his programmers attended the annual DMEXCO conference on digital advertising, where thousands of people from different parts of the digital advertising industry congregate each year. Following the conference, the defendant contacted the U.S. fraud detection firm Integral Ad Science whose representatives had been present at the conference and requested more information about its fraud detection products, under false pretenses, stating “I want to add your filter to us to get more clean traffic to our advertisers.” In fact, the defendant sought—and obtained—details on IAS’s fraud detection technology in order to reverse-engineer and circumvent it. During the conference, the defendant and his co-conspirator described themselves, in an edited self-taken photo, that they “take on whatever makes money.”

The defendant and his co-conspirators operated the scheme and tracked the performance of the bots through a command-and-control server located at CentByCent.com. The defendant owned CentByCent.com, but hid that fact from public databases by using an anonymization service and further sought to hide that fact from law enforcement by giving the anonymization service the name of another individual (Roman Davydov) whom the defendant termed his “fake director.” The CentByCent.com command-and-control server provided instructions and resources to the thousands of bots, received statistics back from the bots regarding the number of fraudulent ad impressions being generated, and forwarded that information to the defendant and his co-conspirators. Screenshots and photographs of CentByCent.com were found in the defendant’s devices and electronic storage accounts, and the defendant’s browsing history indicated that he visited CentByCent.com multiple times a day.

Overall, over the course of the scheme, the defendant and his co-conspirators falsified billions of ad impressions and made millions of dollars. For example, during a single day in October 2016, the defendant and his co-conspirators recorded more than \$56,000 in revenue from placing more than 442 million fraudulent bid requests and falsifying more than 16 million ad impressions. Hundreds of brands and ad agencies around the world collectively paid more than \$7 million in advertising fees for fraudulent ad traffic. The defendant, in turn, reaped millions of dollars in revenue.

The defendant directed and transferred proceeds from the scheme to and through multiple personal and corporate bank accounts located around the world. This included at least four personal bank accounts and at least six corporate bank accounts, located in Bulgaria, Russia, the United Kingdom, the Czech Republic, Latvia, and Cyprus. In the course of opening at least one of these accounts, the defendant lied to the bank about the nature of his business, falsely claiming that it was an “Advertising platform” engaged in “traffic arbitration” which “is the purchase of traffic from some sources/systems (ad exchange) and forwarding it to other sites or affiliate programs.” GX 301T. The defendant re-invested some of the proceeds from the scheme to perpetuate the fraud, including to pay for servers and IP addresses used in the scheme. He explained: “we take a thousand .. spend

it to buy 1000 proxies and 4 servers .. this bundle gives us a 2000/month profit ... out of it, we keep 1000 for the next month to buy proxies and servers again ... and split a thousand.” GX 1678TE.

On December 20, 2016, researchers at White Ops, a private cybersecurity firm based in New York City, publicly revealed the operation of the scheme in a white paper titled “The Methbot Operation.” In the white paper, White Ops revealed a list of IP addresses of computers used to carry out the scheme (the “Methbot IPs” (GX 1)). Following public disclosure of the scheme, the defendant and his co-conspirators reacted by attempting to delete evidence, including communications exchanged between and among co-conspirators. For example, they deleted more than 26,000 emails from the adw0rd.yandex.ru@gmail.com email account associated with the scheme, which was identified in the white paper and which was the registration email account for more than 1,400 IP addresses used in the scheme. On December 23, 2016, the defendant deleted records from his ibetters2@gmail.com account, which he also used to perpetrate the scheme. GX 1709T. The defendant also deleted the Methbot code and logs from the datacenter computer servers that he had rented in the U.S. (GX 103, GX 104), and various LinkedIn messages associated with the scheme (GX 683). On December 24, 2016, the defendant deleted four servers associated with the scheme, including servers used to host MediaMethane.com and CentByCent.com (GX 410, GX 411A).

The scheme deceived and victimized numerous businesses in the digital advertising industry. The scheme victimized hundreds of brands who sought opportunities to advertise their goods and services to real human internet users but lost those opportunities and instead paid for advertisements automatically loaded by computers. These brands included Pepsi, Purina, GlaxoSmithKline, and the Texas Scottish Rite Hospital for Children. Google, which provides advertising services for individuals and businesses, identified hundreds of U.S. companies who, collectively, paid more than \$7 million for Zhukov’s fraudulent ad traffic. GX 1503.

The scheme victimized more than 6,000 online publishers (GX 6), by creating false and fraudulent webpages purporting to be located at real publishers’ domains, stealing the publishers’ identities and misappropriating those identities for a fraudulent purpose, undermining the reputation and credibility of those publishers in the ad market and reducing the revenues that the actual publishers would otherwise earn. These publishers included the New York Times and the New York Post.

The scheme victimized the SSPs and DSPs (“ad platforms”) by causing them to receive false information indicating that a real human user had viewed an advertisement on a real website. These platforms included Google and AdKarma.

The scheme also victimized internet service providers by stealing their corporate identities for the purpose of registering IP addresses with false information (including Comcast, Charter Communications/Time Warner Cable, and others listed in GX 525A); fraud detection firms DoubleVerify (GX 1568A), Forensiq (GX 1573), Integral Ad

Science, TubeMogul, FraudLogix, MOAT, SpringServe, and WhiteOps (and their clients); and internet registries and databases, including AFRINIC and Maxmind, to whom the defendant sent false information about the IP addresses he controlled.

The defendant specifically targeted American and New York-based companies. This was not accidental: in one chat communication introduced at trial, a co-conspirator joked that the Russian government should give the conspirators “a medal for the disruption of the competitor’s economic power”—referring to U.S. economic power. GX 625T. The defendant responded, “SPOT ON!” *Id.* Additionally, when fraudulently registering IP addresses to mask the source of the defendant’s fraudulent traffic—datacenters in Dallas and Amsterdam—and make it appear that the traffic was originating from human users throughout the United States, the defendant specifically targeted New York City. GX 614E; Tr. at 2068-2071 (defendant instructs a third party to register IP addresses as “Verizon Trademark Services, LLC” and asks “can you also change one block to different city? New York is the best!”).

The defendant was arrested in Varna, Bulgaria on November 6, 2018.

Guidelines Calculation

I. The Guidelines Range

The government submits that the Court should apply the Guidelines calculation set forth below, which results in a total offense level of 37 and a criminal history category of I, producing an advisory range of 210 to 262 months’ imprisonment. This calculation is primarily driven by the grouping of the defendant’s convictions for wire fraud conspiracy, wire fraud, money laundering conspiracy, and money laundering, and various enhancements as follows:

Base Offense Level (§§ 2S1.1(a)(1), 2B1.1(a)(1))	7
Plus: Loss Exceeded \$3,500,000 (§ 2B1.1(b)(1)(J))	+18
Plus: Involved 10 or More Victims (§ 2B1.1(b)(2)(A))	+2
Plus: Substantial Part of the Fraudulent Scheme Committed From Outside the United States and Involved Sophisticated Means (§ 2B1.1(b)(10))	+2
Plus: Defendant was Convicted of an 18 U.S.C. § 1956 Offense (§ 2S1.1(b)(2)(B))	+2
Plus: Defendant was an Organizer or Leader (§ 3B1.1(a))	+4
Plus: Obstruction of Justice (§ 3C1.1)	<u>+2</u>
Total:	<u>37</u>

The foregoing calculation reflects the calculation set forth in the PSR, minus the enhancement for possession and use of an authentication feature, which the government agrees does not apply in this case. See PSR ¶¶ 48-49, 55-69, 104.

II. The Defendant's Objection to the Loss Amount Is Without Merit

The defendant's objection to the loss amount is without merit and is merely an attempt to minimize his conduct. The defendant contends that the 18-level enhancement based on an estimated loss of \$7.6 million should not apply because, he alleges, it is "based on conjecture about the source of the traffic." See Deft. Mem. at 10-14. This argument ignores the trial evidence.

The government introduced evidence at trial of a list of IP addresses associated with the defendant's fraud—GX 1 (the "Methbot IPs"). White Ops Senior Director for Detection Dimitrios Theodorakis testified about the data associated with the Methbot IPs and explained why the computers registering ad impressions from those IPs all belonged to the same scheme and to the same bad actor. See Trial Tr. 688-89 (testifying about the White Ops logs for the ad impressions coming from the IPs in GX 1, which were "classified as Methbot"); GX 1 ("IP ranges identified as being used by the 'Methbot' ad fraud operation from October 2016 through December 2016").

Mr. Theodorakis explained how the ad impressions emanating from the Methbot IPs shared the same unusual characteristics or red flags. For example, Mr. Theodorakis explained that White Ops collected copies of the webpages where ads were loading, and that for the computers registering ad impressions from the Methbot IPs, all of the webpages were empty pages with the word "Meth" embedded in the code. Trial Tr. 698-700, 721-23 (the "samples of web pages that we saw from these IPs and one of the functions had the name meth and it was in every single sample of pages that we collected, the meth word was everywhere"; "the traffic we were seeing from these IPs consistently had the characteristics of meth in the pages that were being rendered"; "the highlighted section includes the word meth and that was consistently what we were observing from these IPs"). The Methbot IPs also shared other red flags, including: mismatched ISP/ASN information that was mismatched in a specific way (where the ISP signified a residential internet provider but the ASN signified a datacenter); round-the-clock internet activity with a spike around 8:00 a.m.; a consistent setting of Eastern time zone; certain esoteric browser versions not in common use; a pattern of rapid and voluminous mouse movements; a specific typo in the browser plugins; and no supported voices. See GX 8; Trial Tr. 706-14, 725 (explaining that these shared characteristics amounted to a "fingerprint" of the bot). Therefore, all 1.2 billion ad impressions recorded from the IPs in GX 1 were classified as nonhuman and all of them were classified as Methbot. Trial Tr. 715-16, 754.

Per Bjork, a group product manager at Google who works on its ad traffic quality team, explained that he analyzed Google's own logs for the ad impressions emanating from the Methbot IPs and his observations corroborated the finding that those ad impressions were all generated by the same bot. Trial Tr. 2466, 2489-93 (explaining that the ad impression activity from the Methbot IPs all shared the same red flags); Trial Tr. 2493 ("The traffic from all these IP addresses were very consistent and it looks like they were from the same source.").

Lena Loewenstine, a computer scientist for the FBI, testified about her analysis of one of the defendant's 2,000 servers and tied the Methbot IPs to the defendant in several ways. Ms. Loewenstine testified that she "found IPs in several different places on the drive, in the database, in the logs; and [she] also found some files that were part of the code that also contained some IP information" and "almost all of the IPs I found on the drive matched this list of IPs from White Ops" that was GX 1. Trial Tr. 616-17.

Business records and communications in the case also tied the Methbot IPs to the defendant and reflected extensive cross-corroboration from different evidentiary sources showing that the defendant controlled the IP addresses listed in GX 1. See, e.g., GX 209, 210, 211, 231 (IP leasing company letters of authorization issued to the defendant giving him the exclusive right to use the listed IP ranges); GX 1802, 1803, 1804, 1805, 1806 (AFRINIC registration records for IP ranges the defendant registered with AFRINIC); GX 525A, 525B, 525C, 525D, 525E, 525F, 525G, 525H, 525I, 525J, 525K (Domain Tools registration records for IP ranges in the defendant's email and stolen corporate names); GX 614E (defendant discussing registration of IPs in MaxMind); GX 1549 (fraud monitoring report exchanged with Denisoff listing IPs).

The defendant argues that Ms. Loewenstine's testimony "casts doubt on the reliability of IP addresses to determine [] the source of internet traffic" because she testified that IP addresses could be spoofed. Def. Mem. at 11. In making this argument, the defendant misleads by selectively quoting the record. Despite the defendant's repeated efforts to inject confusion into the record on this point, Ms. Loewenstine was quite clear on how the defendant's servers sent traffic from the IPs listed on GX 1. Ms. Loewenstine explained that the browser on the defendant's bot servers consulted a master database of IPs hosted at the defendant's command-and-control server (centbycent.com), and the browser would then "set the IP [of the bot server] to whatever IP it had chosen from the database." Trial Tr. 604-05. Ms. Loewenstine found these so-called "proxy" IPs in several different places on the server she analyzed:

[The IP addresses that she found on the defendant's server] were used to launch the Methanum browser. They were used when the browser was trying to connect. It was – it was being set and when it would make a connection on the internet, the IPs that I compared to this list were being used in the browser to make it look like traffic was coming from that – those IPs. . . . [I]t spoofs that the traffic was coming from these IPs. . . .

The Government Exhibit 1 is a list of IPs that's White Ops'. When they look at traffic that they obtained from Methbot, they were making a list [that] was all the IPs that they saw the traffic coming from.

So the way the code works, when it[] sent communications on the internet, it would say it's coming from an IP that was not the true IP of the drive. So, WhiteOps would not see that true IP. They

would see these other IPs that the code is pretending the traffic is coming from.

Trial Tr. 624, 626. This scheme worked because the defendant controlled both the true IPs of the servers and the proxy IPs that the browser used to disguise the servers.

The defendant argues that Mr. Bjorke’s testimony “casts even further doubt on the reliability of the loss amount calculated” because, the defendant contends, it is unclear whether the advertisers “actually paid” the entire \$7.6 million listed in Google’s table of losses and whether Google then refunded the money back to the advertisers. The Court need not engage on this question because it is legally irrelevant whether the money actually went out the advertisers’ doors and whether Google refunded it—loss amounts under the Guidelines account for both actual and intended loss, and so the defendant’s failed attempts to obtain money from the victims are well within bounds. See U.S.S.G. § 2B1.1(b)(1) and Application Note 3. In any event, the defendant once again misleads by selectively quoting the record. Mr. Bjorke testified that the amounts listed in GX 1503 were “the total cost of the advertising space” that advertisers bought, that “[m]ost of this was paid to sellers because most of the traffic had happened before December,” that “it’s possible that a portion of this amount were corrected during December, and therefore, was not invoiced because we were able to make adjustments before we sent them the invoice for December,” and “I know the majority of this was invoiced, but there’s a possibility about 10 to 15 percent was not invoiced.” Trial Tr. 2569-71. Given those additional details, even if the ultimate money flow were relevant for the loss calculation (which it is not), and even limiting the loss calculation to the amount “actually paid,” the actual losses are at least \$6.4 million, subjecting the defendant to the same 18-level Guidelines enhancement.²

Therefore, the 18-level enhancement for loss amount is supported by specific, credible, unrefuted evidence and is not speculative—in other words, it is a reasonable estimate based on the available information. See U.S.S.G. § 2B1.1 Application Note 3(C) (district court “need only make a reasonable estimate of the loss . . . based on available information” and “the court’s loss determination is entitled to appropriate deference”).

The defendant cites cases from the drug context to suggest that more is required, Def. Mem. 12-13, but those cases are inapposite because the Second Circuit has rejected the

² The defendant proposes an alternative loss amount based solely on transactions involving Plexious. This calculation drastically understates the loss in this case. Any alternative loss calculation must take into account all of the defendant’s transactions with Plexious, Verta Media, and Ad Karma, at a minimum, as the defendant obtained money from each of these entities in exchange for providing “advertising” services—which he obviously did not provide, since the ads were never shown to real human beings—and therefore received fraudulent proceeds from all three of these entities. The government presented evidence at trial summarizing reams of bank records that showed that the defendant received more than \$3.5 million in proceeds from these three entities alone. See GX 348; see also U.S.S.G. § 2B1.1 Application Note 3(B) (court may use gain as an alternative measure of loss if loss cannot reasonably be determined).

reasoning of those cases in the fraud context. See United States v. Bryant, 128 F.3d 74, 75 (2d Cir. 1997) (“In establishing sentencing tables that tie a defendant’s offense level to the amount of loss caused by his offense . . . the Guidelines do not require that the sentencing court calculate the amount of loss with certainty or precision.”); United States v. Coppola, 671 F.3d 220, 249-50 (2d Cir. 2012) (the “evidence need not . . . establish loss with absolute precision”); see, e.g., id. at 250-51 (inferring loss amount based on defendant’s lifestyle).³

III. The Guidelines Calculation is Fair

The defendant argues that the Guidelines calculation, and specifically the enhancements for the loss amount and other specific offense characteristics, overstate the defendant’s level of criminal culpability. Def. Mem. at 16. That is not so, for several reasons.

First, the loss amount proposed by the government and the Probation Department is actually a conservative estimate and understates both the actual and intended losses in this case. This is because the loss amount—\$7.6 million—is based only on Google’s actual losses for the year 2016. This number is limited in three ways: (i) it only accounts for the ad impressions that traversed Google’s platform, which is an undercount because Google does not intermediate every ad impression on the internet and the defendant’s wide-ranging bot traffic was not limited to interactions with Google; (ii) it only accounts for the fraudulent ad impressions that registered successfully (i.e., 40% of the Methbot impressions that Google recorded), which is an undercount because there were also fraudulent ad impressions that the defendant attempted but ultimately failed (i.e., 60% of the Methbot impressions that Google recorded); and (iii) it only accounts for the year 2016, which is an undercount because the defendant’s scheme began in 2014. See Trial Tr. 2486, 2554, 2564, 2570.

The Court would be well within its discretion to use the \$7.6 million number as a basis to extrapolate the full intended losses (to include all attempts) and at least two years of activity. See Bryant, 128 F.3d at 76 (“it is permissible for the sentencing court, in calculating a defendant’s offense level, to estimate the loss resulting from his offenses by extrapolating the average amount of loss from known data and applying that average to transactions where the exact amount of loss is unknown”). Were the Court to make a reasonable estimate of all intended losses for 2016 recorded at Google, it would arrive at a loss amount of \$19.1 million (resulting in a Guidelines range of 262 to 327 months). Were the Court to further increase that number to estimate cumulative losses for the entire duration of the scheme, it would exceed the next loss amount threshold of \$25 million (resulting in a Guidelines range of 324 to 405 months).

³ For example, although the Second Circuit rejected extrapolating drug quantities based on averages in the drug context, see United States v. Martinez (cited in Def. Mem. at 12-13), the Second Circuit upheld extrapolating loss amounts based on averages in the fraud context, stating, “it is permissible for the sentencing court, in calculating a defendant’s offense level, to estimate the loss resulting from his offenses by extrapolating the average amount of loss from known data and applying that average to transactions where the exact amount of loss is unknown,” Bryant, 128 F.3d at 76.

The government has not sought for such ranges to apply, even though the facts and the law support them. Rather, the government has proposed a concrete and conservative loss amount of \$7.6 million that represents actual losses to advertisers directly resulting from fraudulent Methbot traffic, as documented in extensive and detailed logs kept by a leading advertising platform. In doing so, the government has arrived at a Guidelines calculation that represents a middle ground, and the Guidelines calculation is not only fair, but generous to the defendant.

Despite the government applying a conservative estimate of the loss amount, the loss enhancement remains significant, and that is for one simple reason—because the defendant perpetrated a massive fraud across the entire digital advertising industry affecting thousands of companies across the United States, and not because of any flaw in the Guidelines. Indeed, this conservative estimate of loss is remarkable for its restraint. It makes no pretense of measuring the harm to business-men and -women attempting to operate in good faith in the industry; the damage to the reputations and credibility of individuals and businesses caught in the middle holding the bag for the defendant’s deceit; the time, effort, and expense incurred by companies attempting to unravel the false information and unwind the transactions related to them; or the damage done to the trust and confidence in commercial relationships essential to making the digital advertising industry work and supporting the free and open internet. See United States v. Mohammed, 315 F. Supp. 2d 354, 358 (citing similar harms in connection with credit card fraud and noting that “[n]o simple calculation of dollar ‘loss’ will adequately measure the seriousness of this crime”).

Second, the defendant’s argument that the Guidelines range related to fraud offenses is the subject of long-standing criticism and not a legitimate benchmark is misplaced in this case. The concerns expressed by courts with respect to the fraud Guidelines refer to select circumstances where the loss amount does not correlate to the extent of actual victimization. See, e.g., United States v. Corsey, 723 F.3d 366, 368 (2d Cir. 2013) (wire fraud defendant’s loss enhancement based on “conspiracy to defraud a non-existent investor of three billion dollars”); United States v. Emmenegger, 329 F. Supp. 2d 416, 427 (S.D.N.Y. 2004) (securities fraud defendant’s loss enhancement based on “a kind of accident” related to a single victim’s security procedures); United States v. Johnson, No. 16-CR-457, 2018 WL 1997975, at *3 (E.D.N.Y. Apr. 27, 2018) (wire fraud defendant’s loss enhancement based on gain from fraudulent trades).

Those same concerns—of loss being untethered to concrete victimization—do not pertain to this case. As explained above, the loss amount in this case represents actual losses to advertisers reported by one advertising platform for one year of a multi-year fraud—which place the defendant in the Guidelines category of losses exceeding \$3.5 million. There is no injustice in holding the defendant accountable for losses exceeding \$3.5 million: these losses represent real U.S. dollars that went out of the bank accounts of real U.S. companies—not contingent or hypothetical losses—and the government proved that the defendant gained at least that much in proceeds from the scheme. See supra n. 1.

This is a far cry from the circumstances of the case on which the defendant primarily relies—the concurring judge’s opinion in United States v. Corsey, 723 F.3d 366, 377 (2d Cir. 2013). Corsey involved a defendant who engaged in what the court characterized as a

“ridiculous” fraud involving “a purported coalition of Buryatian nationals and Yamasee tribesmen using AOL email accounts to offer five billion dollars in collateral for a loan to build a pipeline across Siberia.” 723 F.3d at 377. The target of the scam, who quickly recognized that “the deal smelled,” only continued to pursue the transaction because he was working as an informant for the government. *Id.* at 369-70. Under these circumstances, the Second Circuit recognized “the low risk that any actual loss would result” and expressed concerns that the district court had not sufficiently considered whether the Guidelines, which called for a life sentence, overstated the seriousness of the offense. *Id.* at 377. Unlike *Corsey*, the fraud in this case was all too real. The defendant flooded the online advertising industry with fake goods in the form of billions of ad impressions, and hundreds of U.S. companies were collectively defrauded of millions of dollars as a result. In addition to the actual losses recorded, the presence of the defendant’s bots required companies across the industry to spend significant sums of their own money to protect against fraud, and injected risk and undermined confidence in the marketplace.

Indeed, there are plenty of cases in which defendants engaged in complex frauds with Guidelines ranges at the high end of the scale nonetheless received severe sentences. *See United States v. William Lange*, No. 10-CR-968 (E.D.N.Y.) (defendant convicted of conspiracy to commit wire fraud and conspiracy to commit wire fraud and securities fraud, had a Guidelines range of 210 to 262 months, and was sentenced to 262 months’ imprisonment); *United States v. Eric Aronson*, No. 12-CR-245 (E.D.N.Y.) (defendant convicted of securities fraud, had a Guidelines range of 292 to 365 months, and was sentenced to 124 months’ imprisonment); *United States v. George Porrata*, No. 16-CR-093 (E.D.N.Y.) (defendant convicted of conspiracy to commit securities fraud, his Guidelines range was capped by the statutory maximum of 60 months, and was sentenced to 60 months’ imprisonment); *United States v. Jason Galanis*, No. 16-CR-371 (S.D.N.Y.) (defendant convicted of securities fraud conspiracy, investment adviser fraud conspiracy and securities fraud, had a Guidelines range of 188 to 235 months, and was sentenced to 173 months’ imprisonment); *United States v. Pedro Jaramillo*, No. 17-CR-004 (S.D.N.Y.) (defendant convicted of commodities fraud and wire fraud, had a Guidelines range of 78 to 97 months, and was sentenced to 144 months’ imprisonment); *United States v. Philip Kenner*, No. 13-CR-607 (E.D.N.Y.) (defendant convicted of wire fraud conspiracy, wire fraud, and money laundering conspiracy, had a Guidelines range of 262 to 327 months, and was sentenced to 204 months’ imprisonment).

Third, the defendant’s argument that the specific offense characteristics are overlapping and unfairly enlarge the Guidelines range is also misplaced in this case. “The imposition of somewhat overlapping enhancements does not necessarily mean double counting has occurred. Indeed, double counting is legitimate where a single act is relevant to two dimensions of the Guidelines analysis.” *United States v. Samet*, 200 F. App’x 15, 24 (2d Cir. 2006) (internal marks and citations omitted). Here, the defendant’s scheme had numerous dimensions that more than warrant the three specific enhancements that apply: the scheme victimized hundreds of advertisers and thousands of publishers in the digital advertising industry; it was carried out through the use of extremely sophisticated computer technology and infrastructure located throughout the world; and funds were raised for the scheme, and reinvested from the scheme, through shell companies and bank accounts throughout the world, to continually expand its scope and effect. *See Samet*, 200 F. App’x at 24 (no impermissible

double counting where use of sophisticated means was not unique to money laundering activities but was also used to accomplish the underlying frauds); United States v. Hatala, 552 F. App'x 28, 30-31 (2d Cir. 2014) (no impermissible double counting where sophisticated means enhancement was justified by defendant's intricate and complex computer programming and loss amount enhancement was justified by significant monetary damage inflicted).

Moreover, the application of the specific offense characteristics is not so commonplace that they should fall out of the analysis altogether. Each of the enhancements applies in only a portion of fraud cases. See United States Sentencing Commission, Use of Guidelines and Specific Offense Characteristics (2020) (attached hereto as Exhibit A). They are thus useful for distinguishing among the array of frauds prosecuted at the federal level, and warranted in the specific circumstances of this case. See Samet, 200 F. App'x at 24 (rejecting Lauersen-based argument that district court should have downwardly departed based on "combined effect of substantially overlapping offense level adjustments and the increased extent of enhancement of the applicable sentencing range that occurs at the higher end of the sentencing table," where challenged enhancement does not substantially overlap with other offense level adjustments and the defendant "merely seeks to eliminate the effect of the enhancement based on the significant effect it would have on his sentence, which the district court did not have to do").

Fourth, the most recent version of the Guidelines already takes into account the criticisms voiced by prior jurists regarding the enhancements in fraud cases.

In 2015, the Sentencing Commission underwent the process of amending the fraud Guidelines. In doing so, and as part of its extensive notice-and-comment procedure, the Commission considered a multitude of views and data, including the views of those who called for a reduced emphasis on loss amounts and multiple specific offense characteristics. The current Guidelines reflect the result of that considered process. Therefore, the defendant is simply wrong when he argues that the fraud Guidelines do not take account of empirical data and national experience—they expressly do. See Amendments to the Sentencing Guidelines, United States Sentencing Commission (Apr. 20, 2015), at 24 (amending § 2B1.1 "to better account for harm to victims, individual culpability, and the offender's intent"; "This amendment is a result of the Commission's multi-year study of § 2B1.1 and related guidelines, and follows extensive data collection and analysis relating to economic offenses and offenders. Using this Commission data, combined with legal analysis and public comment, the Commission identified a number of specific areas where changes were appropriate."); Chief Judge Patti B. Saris, Chair, United States Sentencing Commission, Remarks for Public Meeting at 2 (Jan. 9, 2015) (noting that the Commission held a symposium on the fraud Guidelines in 2013 at the John Jay College of Criminal Justice, the Commission staff had "spent countless hours analyzing data on fraud sentences," the Commission staff had met with judges and the ABA); see also United States v. Moose, 893 F.3d 951, 958 (7th Cir. 2018) (defendant's "argument that the loss enhancements are not based on the Commission's institutional expertise is mistaken. Even if the enhancements may lack robust empirical support related to deterrence, they have foundations in empirical data and national experience related to the goals of fair sentencing and retribution").⁴

⁴ The cases the defendant cites from the crack cocaine context have no relevance here—in formulating the Guidelines for those offenses, the Commission looked to the mandatory

The current fraud Guidelines remain as they do because—according to Chief Judge Saris who was the Chair of the Sentencing Commission at the time—the Commission’s “extensive process” led it “to believe that the fraud guideline may not be fundamentally broken for most forms of fraud,” Saris, Remarks for Public Meeting at 2, and according to Justice Breyer—who was a member of the original Sentencing Commission before he joined the Supreme Court—the Commission sought “to avoid unfair anomalies” and “increase certain ‘white collar’ sentences when necessary to avoid disparity between ‘white collar’ and ‘blue collar’ crime,” Justice Stephen Breyer, *Federal Sentencing Guidelines Revisited*, 11 Fed. Sentencing Reporter 180, 181 (1999). The Guidelines range in this case—210 to 262 months—does just that, by advising a sentence that is comparable to the sentences of street criminals who commit non-violent thefts from large institutions:

- United States v. Robertson, 837 F. App’x 61 (2d Cir. 2020) (120-month sentence substantively reasonable for defendant who robbed two Subway sandwich stores and three bank branches and stole a total of \$10,532; defendant pleaded guilty to one count of bank robbery; Guidelines were 151 to 188 months).
- United States v. Cascio, 771 F. App’x 91 (2d Cir. 2019) (180-month sentence substantively reasonable for defendant who robbed bank of \$306; defendant convicted after jury trial of bank robbery and entering a bank to commit a larceny; Guidelines were 210 to 240 months).
- United States v. Arrington, 94 F. App’x 858 (2d Cir. 2004) (180-month sentence substantively reasonable for defendant who robbed bank of \$1000; defendant pleaded guilty to one count of bank robbery; Guidelines were 151 to 188 months).⁵

The fact that the defendant had the means to commit his theft with the benefit of technological skill, seed money, and connections to other cybercriminals—using computer servers instead of demand notes—does not exempt him from severe punishment or render the Guidelines unfair. See Moose, 893 F.3d at 958 (noting that the fraud Guidelines “reflect the Commission’s policy judgment that increasing sentences for white-collar crimes would promote greater respect for the rule of law”).

In sum, the circumstances presented here do not warrant a summary rejection of the Guidelines range as a matter of policy. See United States v. Qualls, 25 F. Supp. 3d 248, 259-

minimum sentences set by Congress, did not take account of empirical data and national experience, and itself reported that the crack/powder disparity produced disproportionately harsh sanctions. See Kimbrough v. United States, 552 U.S. 85, 105 (2007). That is not true for the fraud and money laundering Guidelines—those Guidelines are not tethered to any mandatory minimum, they account for empirical data and national experience, and have not been renounced by the Commission itself in any way.

⁵ In each of these cases, the crime of conviction was a note robbery and the defendant did not have a gun. In the last two cases, the defendants had a history of substance abuse.

60 (2d Cir. 2014) (declining to reject the Guidelines range as a policy matter); see also United States v. Brunson, 482 F. App'x 811, 821 (4th Cir. 2012) (“while it is true that a district court may vary from Guidelines ranges based solely on policy considerations, including disagreements with the Guidelines, it is equally true that a district court is not required to do so”) (citing various circuits). Rather, the Guidelines properly serve as a useful anchor and benchmark in the circumstances of this case. See Gall, 552 U.S. at 49 (instructing district courts to treat the Guidelines as the “starting point and the initial benchmark”).

Sentencing Law

The standards governing sentencing are well-established. In United States v. Booker, 543 U.S. 220 (2005), the Supreme Court rendered the Guidelines advisory, and emphasized that a sentencing court must consider both the Guidelines and the 18 U.S.C. § 3553(a) factors when making a sentencing decision. Id. at 264; see also United States v. Kimbrough, 552 U.S. 85 (2007).

Although the Guidelines are no longer mandatory, they continue to play a critical role in trying to achieve the “basic aim” that Congress sought to meet in enacting the Sentencing Reform Act, namely, “ensuring similar sentences for those who have committed similar crimes in similar ways.” Booker, 543 U.S. at 252; see also United States v. Crosby, 397 F.3d 103, 113 (2d Cir. 2005) (“[I]t is important to bear in mind that Booker/Fanfan and section 3553(a) do more than render the Guidelines a body of casual advice, to be consulted or overlooked at the whim of a sentencing judge.”). “[A] district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range,” which “should be the starting point and the initial benchmark.” Gall v. United States, 552 U.S. 38, 49 (2007). The Guidelines range is thus “the lodestar” that “anchor[s]” the district court’s discretion. Molina-Martinez v. United States, 136 S. Ct. 1338, 1345-46 (2016) (internal quotation marks omitted).

After making the initial Guidelines calculation, a sentencing judge must consider the factors outlined in Title 18, United States Code, Section 3553(a), and “impose a sentence sufficient, but not greater than necessary, to comply with the purposes” of sentencing: “a) the need to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for that offense; b) the need to afford adequate deterrence to criminal conduct; c) the need to protect the public from further crimes by the defendant; and d) the need for rehabilitation.” United States v. Cavera, 550 F.3d 180, 188 (2d Cir. 2008) (citing 18 U.S.C. § 3553(a)(2)). Section 3553(a) further directs the Court “in determining the particular sentence to impose” to consider: (1) the nature and circumstances of the offense and the history and characteristics of the defendant; (2) the statutory purposes noted above; (3) the kinds of sentences available; (4) the kinds of sentence and the sentencing range as set forth in the Sentencing Guidelines; (5) the Sentencing Guidelines policy statements; (6) the need to avoid unwarranted sentencing disparities; and (7) the need to provide restitution to any victims of the offense. See 18 U.S.C. § 3553(a).

In light of Booker, the Second Circuit has instructed that district courts should engage in a three-step sentencing procedure. See Crosby, 397 F.3d at 103. First, the Court must determine the applicable Sentencing Guidelines range, and in so doing, “the sentencing judge

will be entitled to find all of the facts that the Guidelines make relevant to the determination of a Guidelines sentence and all of the facts relevant to the determination of a non-Guidelines sentence.” *Id.* at 112; *see also United States v. Corsey*, 723 F.3d 366, 375 (2d Cir. 2013) (“Even in cases where courts depart or impose a non-Guidelines sentence, the Guidelines range sets an important benchmark against which to measure an appropriate sentence.”). Second, the Court must consider whether a departure from that Guidelines range is appropriate. *See Crosby*, 397 F.3d at 112. Third, the Court must consider the Guidelines range, “along with all of the factors listed in section 3553(a),” and determine the sentence to impose. *Id.* at 113.

Argument

The government respectfully requests that the Court impose a sentence consistent with the Probation Department’s recommendation of 15 years’ imprisonment and respectfully submits that such a sentence would appropriately reflect the sentencing factors set forth in 18 U.S.C. § 3553(a).

I. The Nature and Circumstances of the Offense

A sentence of 15 years’ would reflect the serious, sophisticated, and wide-reaching nature of the defendant’s criminal enterprise.

The defendant’s conduct was serious and long-running. He developed a criminal scheme that was illegitimate from the outset and made no pretense of legitimacy—the defendant’s bots were programmed to look like humans, for only one purpose, to deceive others into believing they were humans. The seriousness of the defendant’s operation is particularly acute because, unlike more mundane and traditional schemes involving one-off fraud, the defendant used the power of the internet and sophisticated computer programming to expand the effectiveness of his scheme, direct and manage co-conspirators in different countries, attack businesses from afar, steal millions of dollars, and route those millions through bank accounts in multiple jurisdictions.

The defendant engaged in careful and sophisticated preparation and planning to build and operate the scheme: evidence at trial showed that the defendant researched the digital advertising industry and understood how it worked, chat communications showed that the defendant sought technical advice and information on the methods and means of disguising bot traffic as real human traffic, emails and Skype chats showed that the defendant solicited feedback on where his traffic succeeded in defrauding and where it failed and relayed that feedback to his computer programmers to revise and refine the technology, and computer forensic evidence showed that the defendant set up an infrastructure of computer servers around the world and inserted false information into major public databases relied upon in the industry in order to ensure that the scheme succeeded.

The defendant further took measures to protect his identity and evade detection. He obfuscated his true location by running the scheme from datacenter computer servers in the U.S. and the Netherlands, he used numerous personas, aliases, and alternative email addresses to conduct his criminal activities, he used encrypted applications to communicate with co-

conspirators, and he set up corporate entities and bank accounts in more than six countries to receive proceeds of the scheme. See, e.g., GX 348 at 14-16 (Mintek Group registered in the Seychelles with bank account in Latvia; Must Trade registered in the United Kingdom with bank account in the Czech Republic).

The defendant suggests that his offense conduct was less serious because he committed ad fraud using a datacenter botnet made up of computer servers sitting in a warehouse, and not a residential botnet made up of computers sitting in people's homes. Def. Mem. 6-7. However, the evidence at trial showed that advertisers and others in the digital advertising industry regarded datacenter-based botnets of the type that the defendant used to commit ad fraud just as seriously as residential-based botnets—they are simply two different ways to commit the same fraud. See GX 2200.

II. History and Characteristics of the Defendant and The Need for Specific Deterrence

A sentence of 15 years' is also appropriate in light of the history and characteristics of this defendant.

The defendant's interest in fraud was not one-off or transient. The defendant spent 14 years of his life pursuing various online ventures. Trial Tr. 2752-53. In his own private communications toward the end of this period, he described himself as an "experienced scam artist" and "king of fraud." The defendant then spent two-and-a-half years building and fine-tuning the scheme charged in this case. The defendant's devotion of several years of his life to the instant scheme and his own statements demonstrate that he spent a significant period of time committing fraud, and the defendant's communications with his co-conspirator show that he intended to continue committing fraud were he not caught.⁶ This long-running pattern of conduct—and eagerness to do more—reflects an individual with an unflinching willingness to steal from others. Although the defendant has no official prior criminal history in the United States, it is apparent that he is a longtime fraudster who acted with impunity until this prosecution.

The defendant also engaged in a remarkable pattern of obstruction. After the Methbot scheme was publicly revealed, the defendant deleted servers, emails, and records related to the scheme. After his arrest, the defendant initially attempted to distance himself from the

⁶ Just before the Methbot scheme was publicly revealed, the defendant made secretive plans with one of his co-conspirators to ramp up Methbot and use proceeds from the scheme to further expand their fraud. See GX 1658T (Nov. 26, 2016 email with defendant telling Timokhin: "the balance from AdKarma will get to us and ... we will successfully reinvest it"; "Starting Monday! You are not to use any WhatsApps or Telegrams! You are only to respond to a call from me! And only from the phone! No messengers."; "in December, we will launch it in a brute-force mode"; "My proposal is about taking a risk! Stop dealing with Yegors and let's take a risk like we did two years ago... And as for the balance from AdKarma – we should pour it in and buy, you know what!").

scheme entirely and named another individual as its mastermind. In his most recent and striking display of disrespect for the law, the defendant took the stand at trial, perjured himself without hesitation, and showed complete disregard for his oath and for the truth, appearing to treat the process as some sort of game or yet another gamble. See Trial Tr. 2699 (attempting to explain false registrations in public databases by saying, “if you have a dog, you can call it Verizon”); Trial Tr. 2738 (defendant opting for selective translation of questions); Trial Tr. 2765 (the Court noting “constant giggling at the defense table”); Trial Tr. 2887 (defendant received hand signals from counsel during testimony). The defendant’s most recent conduct—taking the stand and lying to the jury and the Court—instills no confidence that the defendant has learned his lesson.

Even now, the defendant shows no remorse, no acceptance of responsibility, and no recognition of the harm that he has caused. He continues to attempt to deflect blame on others—his co-conspirators, his victims, the industry as a whole—and continues to perpetuate falsehoods disproven at trial. The lack of any remorse—or even any pretense of remorse—causes serious concerns about the defendant’s ability or desire to reform. In these circumstances, the defendant’s lack of remorse, efforts to deflect responsibility, and continued insistence that he has hurt no one and done nothing wrong are a basis for withholding lenience. See, e.g., Robinson v. Heath, No. 12-CV-2116, 2013 WL 5774544, at *11 (E.D.N.Y. Oct. 24, 2013) (Garaufis, J.) (“lack of remorse and failure to acknowledge responsibility consistently have been recognized as constitutionally-permissible factors that courts may take into account in determining an appropriate sentence”) (citing cases); see, e.g., United States v. Jeffers, 505 F. App’x 223, 227 (3d Cir. 2012) (district court may consider defendant’s behavior at trial in imposing sentence).

In addition, the defendant poses a high risk of recidivism in light of where he will go after his incarceration. Once he has served his prison sentence in the United States, he will return to the Russian Federation, where post-release supervision will be completely absent and he will be beyond the reach of U.S. law enforcement. After he is back in his home country, the defendant will once again have access to the computer and criminal networks that enabled him to build his cybercrime scheme in the first place. His demonstrated abilities to obtain tools and advice from online sources, recruit computer programmers and co-conspirators to his cause, and build complex digital infrastructures to commit cybercrime will once again have free reign. It is important for the Court’s sentence to show the defendant that the costs of engaging in these crimes significantly outweigh the benefits he enjoyed for so many years. A substantial sentence of incarceration is needed to provide the defendant with time to reflect upon his crimes, experience the consequences of his criminal conduct, and effectively deter the defendant from repeating his offenses.

The defendant claims that he “did not know that this conduct was illegal.” Def. Mem. at 7. This is disingenuous at best and troubling at worst. The defendant was expressly put on notice that his endeavor was illegal, see DX O-E (“it’s illegal”) and GX 2200 (referencing datacenter-based ad traffic as “criminal activity”), and the evidence at trial—including the defendant’s use of encrypted communications, “cover stories,” and false personas—showed that he understood that it was illegal. The defendant committed this brazen fraud not because he believed it was acceptable or legal, but rather in the belief that he would never be caught. Even if one were to credit the defendant’s claim, it is at most an admission that the defendant believed

lying, cheating, and stealing from others was perfectly acceptable so long as he could find a legal loophole permitting him to escape prosecution for it.

The defendant argues that he should obtain a lenient sentence because of the effects on his family. While a defendant's family circumstances are one factor the Court should consider as part of its § 3553(a) analysis, the law is clear that the very considerations upon which the defendant relies are not proper grounds for a downward departure at sentencing, nor do they weigh heavily in a § 3553(a) analysis. Courts in the Second Circuit "have consistently held that ordinary family responsibilities do not warrant [a downward] departure," in part because "innumerable defendants" could demonstrate that their parental responsibilities will be affected by incarceration. United States v. Johnson, 964 F.2d 124, 128 (2d Cir. 1992) ("Disruption of the defendant's life, and the concomitant difficulties for those who depend on the defendant, are inherent in the punishment of incarceration."). The Guidelines also state that "family ties and responsibilities are not ordinarily relevant" to determining whether a downward departure is warranted. U.S.S.G. § 5H1.6; see also Koon v. United States, 518 U.S. 81, 95 (1996) ("the defendant's family ties and responsibilities" are a "discouraged" basis for a departure (citing U.S.S.G. § 5H1.5)). This is because any imprisonment of any parent or supportive family members has adverse consequences for a defendant's family, and absent extraordinary circumstances, a defendant with a family that will be adversely affected by his sentence should be treated no differently than other defendants with families. For this reason, the Second Circuit has repeatedly overturned a downward departure based on family circumstances, including where a defendant was the parent of small children.⁷ In the context of these other cases, it is

⁷ See, e.g., United States v. Mateo-Ruiz, 112 F. App'x 790, 792 (2d Cir. 2004) (holding that the district court "acted outside of permissible limits" by granting a departure where the defendant was a single mother of a four-year-old); United States v. Madrigal, 331 F.3d 258, 260-61 (2d Cir. 2003) (district court abused its discretion in making a downward adjustment where defendant had six children, the three youngest had "very serious problems," and defendant's parents were having trouble taking care of the children, because "the court did not conclude that [the defendant] was the only person capable of providing adequate care for the youngest children" and there was evidence that "the family as a whole remained cohesive," the older three children were doing well, and defendant's "extended family was also available for caregiving"); United States v. Carrasco, 313 F.3d 750, 756-57 (2d Cir. 2002) (family circumstances were not a basis for departure where the defendant's father was ill and where the defendant provided "some support for his three children" because "being the father of three children is in no sense an exceptional circumstance" and because the defendant's siblings could help financially support the defendant's father); United States v. Ruttner, 4 F. App'x 66, 68-69 (2d Cir. 2001) (holding that the fact that the defendant "has three young children cannot, without more, give rise to a downward departure," and that the defendant "failed to demonstrate that there is anything extraordinary about his family circumstances other than the presence of three young children"); United States v. Cutler, 520 F.3d 136, 164-66, 171-72 (2d Cir. 2008) (downward adjustment not supported where defendant had three children who partially depended on his financial support, a brother who suffered from mental retardation and cerebral palsy, and an elderly mother-in-law, because he was not the primary caregiver for any of them); United States v. Khan, 94 F. App'x

clear that the defendant in this case does not present “extraordinary circumstances” supporting a downward departure either from the Guidelines or as part of the § 3553(a) analysis. The defendant’s dependents are fortunate enough to have other sources of support, and the defendant does not serve as the primary caregiver to anyone. That the defendant helped his friends in their times of need and met his obligations to his family is commendable but not extraordinary. The problem is, despite his capacity to treat those he cares about with decency, he had no qualms about cheating and stealing from people half a world away. Ultimately, any difficulties faced by the defendant’s family as a result of his imprisonment are not caused by this Court; the blame lies solely with the defendant; this is unfortunate, but no more so than in any of the hundreds of other cases in this district and in this circuit in which a spouse, a parent, and a friend decides to commit crimes.

The defendant asks this Court to consider his upbringing and past drug abuse as a basis for mitigation. Def. Mem. 1-2. Whatever economic position the defendant may have been in as a child, that was not his position when he launched the Methbot scheme. He had the ability to raise money from investors, the ability to hire computer programmers, the ability to pour hundreds of thousands of dollars into server and IP address rentals, and the ability to sit at home in his swanky seaside apartment behind multiple computers and devote time to building and perpetrating his scheme. The defendant was far-removed from his childhood, both in time and circumstance, when he committed the crimes of conviction. He was in a position to choose among different ventures, that varied in the extent to which they involved cheating and stealing from others. He chose to cheat and steal. He should be held accountable for that considered choice. See United States v. Vera Ramos, 296 Fed. Appx. 201, 203 (2d Cir. 2008) (affirming guideline sentence despite defendant’s “difficult upbringing” and noting district court’s observation that such circumstances are “almost universal” among defendants).

III. The Need to Reflect the Seriousness of the Offense, Promote Respect for the Law, and Provide Just Punishment

A sentence of 15 years will reflect the seriousness of the defendant’s offenses, promote respect for the law, and provide just punishment. See 18 U.S.C. § 3553(a)(2)(A).

33, 38 (2d Cir. 2004) (holding that the district court erroneously departed from the Guidelines because the record did not suggest that the defendant “was the primary—let alone sole—support of any of the many people that he claims to support”); United States v. Osorio, 305 F. Supp. 2d 319, 322 (S.D.N.Y. 2004) (holding that because “the hardships [the defendant] and his family must now face are no more extraordinary than those faced by any defendant who is sentenced to a term of imprisonment and has a family that depends, in part, on his or her financial support,” and that “there is nothing so extraordinary in this case beyond what may commonly befall the young children of incarcerated defendants”); United States v. Jimenez, 212 F. Supp. 2d 214, 216 (S.D.N.Y. 2002) (holding that family circumstances alone were not grounds for departure where the defendant was “a single mother with three children who will suffer grievously from her absence,” one child had “significant disabilities,” and the defendant’s family, who could care for the children, “are themselves so poor that they have been unable to maintain a household in the United States for their own children”).

The defendant's criminal scheme undermined the innovation and advancements that make up the modern internet and the modern U.S. economy. Computers, the internet, and datacenter-based cloud storage are an integral part of the U.S. economy. The expansion of the open and free internet, and the use of digital advertising as the primary revenue model for publishers online, has brought great benefits to the economy and opened up new opportunities for millions of people—from entrepreneurs and small businesses who sell their goods and services exclusively or predominantly through online advertising, to non-profits and political movements that raise money and awareness through online advertising, to publishers who offer news, maps, videos, information, and other free content to internet users worldwide because their revenue comes from online advertising. See Trial Tr. 88-91 (ad industry expert explaining that “much of the Internet you can visit are free are essentially, free thanks to advertising,” explaining how revenue from online advertising is “[e]xtremely important” for publishers ranging from “mom-and-pop” shops to “larger publications” who all rely on online advertising revenue to various extents, and explaining how online advertisers include “[a]nyone who is trying to sell a good or service or trying to raise funds in someway . . . like Coca Cola” or “the flower shop down the road from your house” or “a political advertisement” or “a charity” and that online advertising is particularly affordable for small businesses and “makes it so that small businesses can grow”). Unfortunately, this digital revolution has also created new and unprecedented opportunities for criminals to steal money on a scale and at speeds that were impossible in the physical world. The internet has opened a new frontier for criminals unbounded by traditional mores and physical barriers. Cybercriminals like the defendant can commit their crimes from around the world without ever facing their victims and can use any number of techniques to conceal their identities.

Ad fraud is a particular menace because it exploits the digital advertising supply chain—which necessarily relies on automated software and numerous middlemen to handle the billions of ad opportunities that need to be filled each minute. See Trial Tr. 81-82, 102 (ad industry expert explaining “the sheer number of opportunities” in online advertising resulting from “every single time someone opens a [web]page” and the need to rely on intermediaries: “The reality today is that publishers, because of the sheer number of people on the Internet, are constantly having trouble selling their opportunities. So they are constantly trying to stay in business. And in order to do that, they have to work with as many ad networks and ad exchanges, SSPs, as they possibly can . . .”). This is a system built on trust. See Trial Tr. 81-82 (ad industry expert explaining the inability of advertisers to validate that an ad has been shown to humans online as compared to validating that an ad has been displayed on TV, on a billboard, or in the subway: “For digital advertising, [every time] an opportunity comes to be, you have to trust a little bit that your ad that you purchased is now showing there.”). Ad fraud exploits this system to siphon dollars away from U.S. companies and into overseas bank accounts that are difficult to trace.

Indeed, the evidence at trial demonstrated that private security companies hired by U.S. companies to identify and block fraudulent traffic were generally unable to do so until two years into the scheme, because of the extensive and sophisticated computer technology fueling the scheme and its ability to fool and circumvent fraud detection software. Even where companies are able to detect such traffic, they are generally without recourse, as the individual behind the fraud is difficult to identify and impossible to pursue through civil litigation. See,

e.g., Trial Tr. 2598 (Google witness explaining that when even when they detected invalid traffic, they could see the platform that was passing that traffic on to Google but “had no available resources” to identify the original source of the traffic).

For this reason, ad fraud is a particularly attractive venture for cybercriminals—with relatively little effort and risk as compared to other types of cybercrime, it can yield high payouts and be used to fuel other cybercrime. See Exhibit B (chart comparing risk and reward of various types of cybercrime).

American businesses and consumers are harmed as a result. Indeed, in a 2016 letter to the Federal Trade Commission, Senators Schumer and Warner wrote about “digital advertising fraud and the associated negative economic impact on consumers and advertisers.” They explained: “Bots plague the digital advertising space by creating fake consumer traffic, artificially driving up the cost of advertising in the same way human fraudsters can manipulate the price of a stock by creating artificial trading volume. In each case, markets highly sensitive to demand signals are manipulated. . . . The cost of pervasive fraud in the digital advertising space will ultimately be paid by the American consumer in the form of higher prices for goods and services.”

Digital advertising fraud in the nature of what the defendant committed thus has real impact—overseas actors use sophisticated technology to cheat the system and steal from American companies, knowing that those companies have little-to-no ability to pursue them. This imposes costs on everyone in the industry—with legitimate businesses at every step in the chain spending large sums to hire private security (the fraud detection filters) and essentially operating at their own risk in the absence of the rule of law. It reduces revenues to businesses large and small, and has a particularly deleterious effect on small advertisers, publishers, and ad networks, who depend to a greater extent on online ad revenue and are less able to absorb the loss; and it imposes costs on consumers. Such crimes also undermine consumer confidence and trust in the systems and networks that make up the internet and in the internet itself—and perpetuate the cynical view that the online world is full of lies and scams where criminals can thrive and legitimate businesspeople operate at their own risk. These harms can only be checked by the significant incarceration of wrongdoers. Those who commit such crimes should be held accountable for them and put on notice that the rule of law applies in cyberspace just as it does on the street and substantial prison sentences, commensurate with the losses and damages caused, await those who violate the law.

IV. The Need for General Deterrence

A sentence of 15 years’ is needed for general deterrence, which is crucial in the realms of international cybercrime and fraud. 18 U.S.C. § 3553(a)(2)(B), (C).

As the circumstances of this case demonstrate, it is all too easy for cybercriminals to profit from cybercrime schemes. Cybercriminals like the defendant can make millions of dollars in a short time period. The lure of such easy money in countries with spotty records of cooperating with U.S. law enforcement is substantial. Many may make the calculation that the

rewards are worth the risk when their government is unlikely to extradite them to face justice in the United States.

At the same time, it is all too difficult for law enforcement to identify and capture international cybercriminals like the defendant. Cybercrimes are extremely difficult to solve. Identifying the mastermind behind the keyboard takes unique investigative expertise and attention to detail. The investigations almost universally require the collection of evidence from sources all over the world.⁸ Electronic evidence often disappears before the legal and diplomatic procedures necessary to retrieve the evidence can be completed. Even when law enforcement successfully identify a cybercriminal, many reside in countries that will not extradite their citizens to face justice in the United States.⁹ It is notable that in this case, five charged defendants remain at large.

In the rare instance in which the United States can bring a cybercriminal of the defendant's stature and significance to justice, the sentence must be significant to afford adequate general deterrence, because other overseas cybercriminals who are contemplating this and other sorts of cybercrimes are capable of weighing the low likelihood of detection and apprehension against the consequences of prosecution. Where the incidence of prosecution is lower, the level of punishment must be higher to obtain the same level of deterrence. Furthermore, the need for general deterrence is greatest in cases involving particularly lucrative and difficult-to-detect cybercrime schemes, such as the one that the defendant designed. Numerous courts have recognized the importance, and appropriateness, of such considerations of general deterrence in determining a sentence. See Harmelin v. Michigan, 501 U.S. 957, 988 (1991) (noting that "since deterrence effect depends not only upon the amount of the penalty but

⁸ As part of this investigation, FBI agents obtained business records and bank records from numerous foreign countries pursuant to multiple treaty requests, including Bulgaria, Latvia, the Czech Republic, the United Kingdom, and Mauritius. Detecting and understanding the defendant's fraud also required careful analysis of voluminous computer code and logs. See Trial Tr. 404 (FBI computer scientist analyzed 17,000 lines of code); Trial Tr. 715 (White Ops logs consisted of 1.2 billion ad impressions); Trial Tr. 2605 (Google logs contained many rows).

⁹ Indeed, even in instances where U.S. law enforcement successfully collects the requisite evidence and identifies the actors at issue, bringing those individuals to justice in a U.S. court poses its own challenges. For this reason, the government commonly announces charges without apprehending any of the charged defendants. See, e.g., United States v. Rafatnejad, No. 18-CR-094 (S.D.N.Y.) (charges announced against nine Iranian nationals who conducted cybertheft campaign against universities and companies to steal research, academic, and proprietary data); United States v. Hua, No. 18-CR-891 (S.D.N.Y.) (charges announced against two Chinese hackers who targeted intellectual property and confidential business information); United States v. Iat Hong, No. 16-CR-360 (S.D.N.Y.) (charges announced against four individuals for insider trading based on hacked information; extradition request for defendant arrested in Macau was denied).

upon its certainty, crimes that are less grave but significantly more difficult to detect may warrant substantially higher penalties”); United States v. Gupta, 904 F. Supp. 2d 349, 355 (S.D.N.Y. 2012) (observing where a crime is hard to detect, “others similarly situated to the defendant must therefore be made to understand that when you get caught, you go to jail”). Moreover, because “economic and fraud-based crimes are more rational, cool and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence.” See, e.g., United States v. Martin, 455 F.3d 1227, 1240 (11th Cir. 2006) (quoting Stephanos Bibas, White-Collar Plea Bargaining and Sentencing After Booker, 47 Wm. & Mary L. Rev. 721, 724 (2005)) (internal quotation marks omitted); United States v. Heffernan, 43 F.3d 1144, 1149 (7th Cir. 1994) (“Considerations of (general) deterrence argue for punishing more heavily those offenses that either are lucrative or are difficult to detect and punish, since both attributes go to increase the expected benefits of a crime and hence the punishment required to deter it.”); United States v. Stein, No. 09-CR-377, 2010 WL 678122, at *3 (E.D.N.Y. Feb. 25, 2010) (Weinstein, J.) (“Persons who commit white-collar crimes like defendant’s are capable of calculating the costs and benefits of their illegal activities relative to the severity of the punishments that may be imposed.”); Sentencing Tr. at 49-51, United States v. Knowles, No. 16-CR-005 (S.D.N.Y. Dec. 6, 2016) (Engelmeyer, J.) (“[F]or hackers who operate from abroad who damage the lives and business interests of Americans by remote means, it will often be hard to law enforcement to catch up with them. It’s an unfortunate reality, but between different legal regimes, limited across-border cooperation among law enforcement, and the inherent challenges of identifying and catching cyberthieves, the difficulty of apprehending an overseas hacker is reality. So it is all the more important that when a hacker from outside the United States is caught, the punishment be meaningful to convey to others who operate from afar, so that even if the likelihood of apprehension may not be great, the consequences will be.”).¹⁰

The significance of the sentence that the Court imposes for general deterrence cannot be overstated. This case has, and continues to be, closely watched—in the English and Russian language press, by those in the online advertising industry, in cybercrime legal circles, and by cybercriminals themselves, including some of the defendant’s technically skilled co-conspirators who remain at large. See Exhibit C (Instagram post by co-defendant Mikhail Andreev after unsealing of indictment). The sentence that the Court imposes will send a message to others here and elsewhere about the seriousness with which the United States treats cybercrime and cyberfraud schemes targeting U.S. companies, the risks entailed in engaging in such schemes, and the consequences that will befall those who do.

¹⁰ Knowles’ Guidelines range was 27 to 33 months and the district court sentenced him to 60 months. It is without question that the defendant in this case engaged in criminal activity that was greater in magnitude, scale, and loss, victimizing U.S. companies across an entire industry, and thus the punishment should be greater.

V. The Need to Avoid Unwarranted Sentence Disparities

A sentence of 15 years would also comport with “the need to avoid unwarranted sentence disparities among defendants.” 18 U.S.C. § 3553(a)(6).¹¹

The defendant cites generalized statistics for federal fraud sentences, which he claims warrant a sentence of three years. These statistics are of limited utility, as they represent mere averages among cases whose fact patterns necessarily vary widely. Indeed, the defendant’s case presents several aspects which are not present in the vast majority of fraud cases, including millions of dollars in actual losses, sophisticated computer technology, widespread impact on the industry, and obstructive conduct.

When considering comparable cases, the Court should take into account both the technical sophistication of the defendant’s scheme and the nature and extent of the fraud that he perpetrated. Accordingly, while there is no perfect analogue to this case, cases involving defendants who led schemes in the realms of cybercrime and financial fraud can be instructive.

In some respects, a useful comparison is international carding schemes, in which overseas cybercriminals traffic in stolen credit card information online, the end user is generally minimally affected because the fraudulent charges are either blocked or reimbursed, and the loss is generally borne by a large corporation or bank that serves as an intermediary in the transaction.

- In United States v. Roman Seleznev, No. 11-CR-070 (W.D. Wa. 2017), the Honorable Richard A. Jones sentenced the defendant to 27 years’ imprisonment following a jury trial. Seleznev operated the Carder.su website, where he trafficked in stolen credit card data and had a laptop computer in his possession with approximately 1.7 million stolen credit cards. Seleznev was arrested in and extradited from the Maldives.
- In United States v. Roman Vega, No. 07-CR-707 (E.D.N.Y. 2013), the Honorable Allyne R. Ross sentenced the defendant to 18 years’ imprisonment, following a guilty plea and failed cooperation. Vega operated the CarderPlanet website, where he trafficked in stolen credit card data, and had a laptop computer in his possession with approximately 500,000 stolen credit cards. He was arrested in and extradited from Cyprus. Vega pled guilty in this district to a cooperation agreement and provided historical information regarding his co-conspirators; he later breached his cooperation agreement by moving to withdraw his plea and contradicting prior statements.
- In United States v. Albert Gonzalez, No. 08-CR-10223 (D. Mass. 2010), the Honorable Patti B. Saris sentenced the defendant to 20 years’ imprisonment,

¹¹ The government refers to the cases discussed in this subsection to inform the Court of other prosecutions that are pertinent to the issues of sentencing disparity. However, the government is mindful that each defendant was sentenced on the unique facts of his or her case and that aggravating or mitigating circumstances in one case may not be present in others.

following a guilty plea and failed cooperation. Gonzalez and his co-conspirators were involved in hacking schemes in which they stole approximately 7,000 credit cards from one company and 45 million credit cards from another. Gonzalez was arrested in the United States.

Fraud cases outside the cybercrime context are also useful reference points. The cases cited below involve fraud defendants who exercised a leadership role in the scheme, used a company or enterprise that engaged in little to no legitimate business as a front to facilitate the fraud, and caused losses that were largely incurred by large institutions, rather than individuals:

- United States v. Wider, 14 Cr. 221 (E.D.N.Y. 2016): the defendant was the president and sole shareholder of a licensed mortgage bank. The defendant and his co-conspirators – which included lawyers, accountants and real estate appraisers – engineered sham, insider transactions, defrauding FDIC-insured banks of loan principal. The defendant would then securitize and sell the sham mortgages to other large financial institutions and investment banks. The scheme caused over \$18 million in actual losses, and the defendant’s bank engaged in no legitimate business outside of the scheme. The defendant was sentenced to 150 months.
- United States v. Confredo, 10 Cr. 5274 (S.D.N.Y. 2008): the defendant purportedly operated a financial services business that served as the vehicle for his bank fraud scheme. Generally, the defendant coordinated the submission of hundreds of fraudulent loan applications to large New York City area banks, such as Citibank, ostensibly on behalf of hundreds of small businesses. Because the named applicants knew that the loan applications were fraudulent, only the lending banks were victimized. Actual losses were approximately \$10 million. The defendant was sentenced to 205 months.
- United States v. Drivas, 10 Cr. 771 (E.D.N.Y. 2013): the defendants operated a phony medical clinic that defrauded Medicare through a kickback scheme. The lead defendant was the owner and lead physician at the facility and caused \$70 million to be billed for medical services that were never performed, medically unnecessary, or performed poorly by unlicensed individuals. The defendant was sentenced to 151 months, which the Second Circuit found to be procedurally and substantively reasonable. See United States v. Wahl, 563 Fed.Appx. 45 (2d Cir. 2014) (summary order) (noting that, even if the defendant’s claim that he provided legitimate services were true, it would not decrease the loss amount enough to alter the total offense level under the Guideline).

VI. The Circumstances of This Defendant’s Incarceration
Do Not Provide a Basis for Significant Mitigation

The defendant argues that the circumstances of his detention at the MDC during the COVID-19 pandemic warrant a downward variance.

COVID-19 has undoubtedly had a significant impact on everyone's lives. In the face of the global pandemic, the MDC modified operations and adopted precautionary measures to safeguard the health and safety of its inmates, staff, and the community at large. The MDC's management of the COVID-19 pandemic has been the subject of litigation, most notably in Chunn v. Edge, No. 20-CV-1590 (E.D.N.Y. June 9, 2020). In that case, Judge Kovner found that MDC officials "recognized COVID-19 as a serious threat and responded aggressively," "recognize[d] their duty to inmates," took "swift and extensive countermeasures," and were neither exhibiting deliberate indifference nor violating any standard of care. Id. The MDC's handling of emergencies has continued to be the subject of litigation, under the supervision of Chief Judge Brodie, and while the defendant cites one report from that litigation, he fails to note that the concerns raised in the report were subsequently addressed during the course of that litigation. See Federal Defenders of NY v. BOP, No. 19-CV-660 (E.D.N.Y.); id., ECF Nos. 130, 134, 139, 143, 145, 151 (biweekly status letters).

Notably, the report that the defendant references (Def. Ex. M) is not specific to the defendant, and the defendant does not claim to have suffered from any of the conditions outlined in the report. Indeed, the defendant was specially positioned at MDC during the pandemic. He received the COVID-19 vaccine in January 2021, before most of his fellow inmates, and before a vast majority of Americans were even eligible. In addition, he received a significant dispensation to depart from his cohort to go to the visiting room on a daily basis and use his own computer—an extraordinary and exceptional accommodation not afforded to the vast majority of other defendants. See ECF No. 284, 284-1 (listing the defendant as one of six inmates in the entire institution with daily privileges to go to the visiting room to review discovery and noting dates that defendant accepted such access and dates that he refused).

Given these circumstances, the defendant was not subject to conditions of incarceration that were unusually harsh as compared to his fellow inmates.¹² See United States v. Murden, No. 20-CR-555 (E.D.N.Y. July 12, 2021) (Matsumoto, J.) (declining to find incarceration at MDC during the pandemic to be a mitigating circumstance justifying downward variance from Guidelines range and imposing middle-of-Guidelines sentence).

¹² This is in contrast to other inmates whose specific circumstances were unusually harsh and, even as to them, the circumstances provided only slight mitigation, not the windfall of time-served that the defendant here seeks. Cf. United States v. Garland Battle, No. 20-CR-349 (E.D.N.Y. Apr. 22, 2021) (Komitee, J.) (where Guidelines range was 30 to 37 months and government requested 21 months, the Court imposed sentence of 27 months in part to account for "harsher than usual" conditions); United States v. Kenner, No. 13-CR-607 (E.D.N.Y. Oct. 5, 2020) (Bianco, J.), Sentencing Tr. at 100-01 (where Guidelines range for fraud defendant was 262 to 327 months and government asked for 240 months, Judge Bianco imposed sentence of 204 months, in part because defendant submitted "pages and pages, almost like a diary, going through each incident with the MDC with the guards" and was given unwarranted SHU time, and in part because defendant was somewhat less culpable than comparable defendant who received 240 months).

Should the Court nevertheless be inclined to consider the defendant's incarceration at MDC as a mitigating circumstance, the government notes that it is not sufficient to justify a sentence substantially below the Probation Department's recommendation, which already downwardly departs from the Guidelines range. Indeed, the Second Circuit has recently cautioned district courts against placing too great reliance on mitigating factors that are inadequate to justify substantial departures from the Guidelines range. See United States v. Ceasar, --- F.4th ---, No. 19-2881, 2021 WL 3640387, at *17 (2d Cir. Aug. 18, 2021) (vacating sentence as substantively unreasonable where district court downwardly departed from Guidelines range of 360-600 months' and imposed sentence of 48 months on account of defendant's need for rehabilitation from years of trauma and abuse, holding that district court erred in giving that fact "overwhelming weight while failing to give adequate consideration to the competing goals of sentencing—including the need for the sentence to protect the public, deter criminal conduct of the defendant specifically and others generally, promote respect for the law, and reflect the seriousness of the offense committed"); United States v. Mumuni, 946 F.3d 97, 108 (2d Cir. 2019) (vacating sentence as substantively unreasonable where district court downwardly departed from Guidelines range of 85 years and imposed sentence of 17 years on account of defendant's youth at the time of the offense, lack of criminal record, and lack of disciplinary infractions during incarceration, holding that those factors could not "bear the mitigating weight [that the district court] assigned to them").

Conclusion

In this case, a sentence consistent with the Probation Department's recommendation of 15 years' imprisonment will appropriately capture the defendant's conduct, account for the need to deter the defendant and other cybercriminals operating overseas, and avoid unwarranted sentencing disparities. The government respectfully submits that such a sentence would be sufficient, but not greater than necessary, to carry out the goals of sentencing set forth in 18 U.S.C. § 3553(a).

Respectfully submitted,

JACQUELYN M. KASULIS
Acting United States Attorney

By: /s/Saritha Komatireddy
Saritha Komatireddy
Artie McConnell
Alexander Mindlin
Assistant U.S. Attorneys
(718) 254-7000

cc: Clerk of the Court (EK) (by ECF)
All counsel of record (by ECF)